



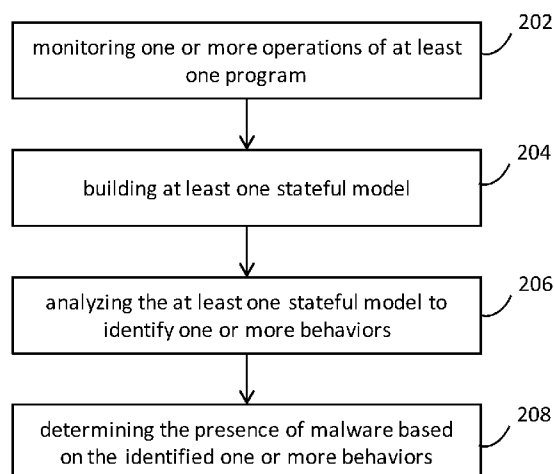
- (51) International Patent Classification:
G06F 21/56 (2013.01)
- (21) International Application Number:
PCT/IL2015/050802
- (22) International Filing Date:
5 August 2015 (05.08.2015)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
14/456,127 11 August 2014 (11.08.2014) US
- (71) Applicant: SENTINEL LABS ISRAEL LTD. [IL/IL]; 24
HaYetzira Street, 5252164 Ramat Gan (IL).
- (72) Inventors: WEINGARTEN, Tomer; 2 Amiel Street,
4924013 Petah Tikva (IL). COHEN, Almog; 56 Bazel
Street, 6274430 Tel Aviv (IL). SHAMIR, Udi; 7 Yosef
Ahronovitch Street, 7634707 Rehovot (IL). MOTIL, Kir-
ill; 58 Rotshchild Street, 4947307 Petah Tikva (IL).
- (74) Agent: HAUSMAN, Ehud; REINHOLD COHN AND
PARTNERS, P.O.Box 13239, 6113102 Tel-Aviv (IL).

- (81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG,
MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM,
PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC,
SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ,
TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU,
TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE,
DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,
LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,
SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: METHOD OF MALWARE DETECTION AND SYSTEM THEREOF



(57) Abstract: There is provided a system and a computer-implemented method of detecting malware in real time in a live environment. The method comprises: monitoring one or more operations of at least one program concurrently running in the live environment, building at least one stateful model in accordance with the one or more operations, analyzing the at least one stateful model to identify one or more behaviors, and determining the presence of malware based on the identified one or more behaviors.

Fig. 2